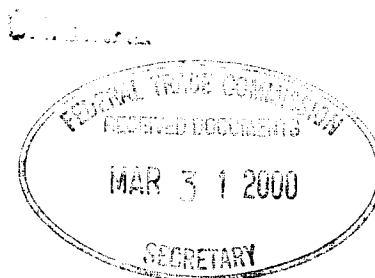




655 16TH STREET, N.W., SEVENTH FLOOR  
WASHINGTON, D.C. 20036-6701  
TELEPHONE: 202-462-6444  
FAX: 202/429-4519  
E-MAIL: FMI@FMI.ORG  
WEBSITE: WWW.FMI.ORG

March 31, 2000



Via Messenger

Secretary, Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

**Re: Gramm-Leach-Bliley Act Privacy Rule; 16 CFR, Part 313: Comments**

Dear Sir or Madam:

The Food Marketing Institute (FMI) respectfully submits the following comments in response to the notice of proposed rulemaking issued by the Federal Trade Commission (FTC) in order to implement the notice requirements and restrictions on the ability of financial institutions to disclose nonpublic, personal information about consumers to nonaffiliated third parties pursuant to Title V of the Gramm-Leach-Bliley Act (GLB Act). 65 Fed. Reg. 11174 (March 1, 2000).

FMI is a non-profit association conducting programs in research, education, industry relations and public affairs on behalf of its 1,500 members and their subsidiaries. Our membership includes food retailers and wholesalers, as well as their customers, in the United States and around the world. FMI's domestic member companies operate approximately 21,000 retail food stores with combined annual sales volume of \$220 billion, which accounts for more than half of all grocery store sales in the United States. FMI's retail membership is composed of large multi-store chains, small regional firms and independent supermarkets. Our international membership includes 200 members from 60 countries.

FMI members have a strong commitment to privacy issues and, in this regard, have developed a policy statement for our industry regarding the use of consumer data, including guidelines on notice, choice, security and access. A copy of our privacy statement is enclosed for your reference.

**A. “Financial Institution” Definition Should Be Clarified To Apply Only to Businesses “Significantly Engaged” in Financial Activities**

Section 509(3) of the GLB Act defines a “financial institution” as “any institution the business of which is engaging in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956.” The FTC has proposed that the “financial activities” referenced in Section 509(3) include not only the traditional financial activities that are specified in Section 4(k) itself, but also those activities that the Federal Reserve Board has found to be “closely related to banking.” See 12 C.F.R. § 225.28. The Federal Reserve Board’s list of activities “closely related to banking” encompasses a broad array of activities, including selling money orders and maintaining financially-related databases. The breadth of the proposed definition would encompass institutions that are not customarily considered “financial institutions” and subjecting these businesses to the proposal at issue would exceed the scope of Congressional intent in enacting the GLB Act.

For example, many supermarkets offer money order sales as a service to their customers in the same way that they cash payroll, personal or government checks. The regulatory list of financial activities also references databases. Many supermarkets maintain internal “bad check” files that they utilize when deciding whether to accept a consumer’s personal check. These files are not shared with third parties and are in no way used to offer traditional financial products.

In the examples cited above, supermarkets are not maintaining deposit accounts, providing consumer access devices for the funds, or engaging in any activity that would customarily be understood as “closely related to banking.” To avoid confusion between those retailers who issue credit, maintain consumer accounts or offer other traditional financial services and those, like most supermarkets, who do not, the Agency should tailor the purpose and scope of the final rule to cover only those institutions who are engaged in activities that are truly “closely related to banking.”

Both the preamble and the proposed rule suggest that the FTC recognizes the problem presented by the broadly drafted regulations. The preamble specifically states that a financial institution must be “significantly engaged” in a financial activity in order to qualify as a “financial institution.” 65 Fed. Reg. at 1176. The preamble further distinguishes between a retail business that offers its own credit cards directly to consumers and a retail business that merely establishes layaway or deferred payment plans. *Id.* at 11177. The proposed rule states as an “example” that an entity is a financial institution if it is significantly engaged in financial activities. Proposed § 313.3(j)(2). Finally, the preamble asks whether the FTC should define “significantly engaged” for purposes of the final rule.

In this regard, the final regulations should be modified in at least two significant ways. First, "significant engagement" in financial activities should be a clearly stated prerequisite to determining whether a business constitutes a "financial institution." Second, "significantly engaged" should be defined by the FTC. The definition should exclude those businesses who offer services that happen to fall into the lengthy list of activities that were determined for other purposes to be "closely related to banking" if those services are only incidental to their core business. *We urge the Commission to state clearly in the final rule that a business, such as a grocery store, that maintains a "bad check" file or provides money orders to its customers, is not "significantly engaged" in financial activities and, therefore, is not a "financial institution" within the meaning of the financial privacy rules.*

**B. "Customer Relationship" Definition Should Be Clarified To Ensure That Use of ATMs in Grocery Stores Does Not Constitute "Continuing Relationship" Sufficient To Transform a "Consumer" into a "Customer"**

The proposed regulations distinguish between "consumers" and "customers" and apply different privacy requirements to each. According to proposed Section 313.4(c), a consumer becomes a customer when "customer relationship" is established, which occurs when the "financial institution" enters into a "continuing relationship" with the consumer.

In defining "customer relationship," the preamble states that using an automated teller machine (ATM), cashing a check, or purchasing money orders at a bank where a customer has no other business would not establish a customer relationship. 65 Fed. Reg. at 11176. The preamble continues to state that, "a consumer would not necessarily become a customer simply by repeatedly engaging in isolated transactions, such as withdrawing funds at regular intervals from an ATM owned by an institution with whom the consumer has no financial account." Id. at 11176.

As you are undoubtedly aware, supermarkets own and operate a variety of ATMs in stores. Some stores do not surcharge customers or else they reimburse the surcharge if the customer makes a grocery purchase. Consumers who wish to avoid ATM charges often utilize these machines as well as the option of surcharge-free cash back at the point-of-sale (checkout lanes) as their primary way of withdrawing funds from their checking accounts. Additionally, grocery stores often offer to cash personal and payroll checks at rates significantly below check cashers and some financial institutions. These services are offered as customer conveniences, not as financial products. Consumers who avail themselves of these "isolated transactions," even if on a repeated basis, should not be construed as having established a "customer relationship" for purposes of this proposed rule.

**C. Financial Privacy Rules Must Not Hinder Development of  
Electronically Converted Check Technology**

In addition to our concerns about the possible scope and definitions in the proposed rule published by the FTC, our industry has also provided comments to the Board of Governors of the Federal Reserve with respect to their financial privacy regulations. Our comments related to how the Federal Reserve's proposed rule might hinder the development of an exciting new payment type: the electronically converted check. We would like to share these comments with the FTC, as well.

The supermarket industry currently accepts hundreds of millions of paper checks annually and the number is increasing each year. We are committed to finding less expensive, more efficient alternatives to the paper check and other forms of payment. Toward this end, we have been in the forefront of efforts to develop "converted checks."

A converted check is a paper check that is presented by the customer to the retailer for payment and then converted to an Automated Clearing House (ACH) transaction at the point-of-sale (POS). The store's POS equipment reads the magnetic ink character recognition (MICR) line on the customer's check and initiates an ACH transaction for the amount of the customer's order. The customer then signs a receipt (similar to a credit card receipt) authorizing the transaction amount to be debited electronically from the customer's checking account via the ACH system. The paper check, which has now been voided so it cannot be used again, is then returned to the customer along with a copy of the signed authorization.

The concern we have with the potential application of this proposed rule is on the back end of the check conversion process. Currently, if an account has insufficient funds to cover the amount of a check at the time that the paper check is presented, the paper check is returned to the retailer by the financial institution. Using the name, address and telephone information printed on the face of the check, the retailer can contact the consumer to make other arrangements to collect payment for the order or to resubmit the paper check for payment. Similarly, supermarket retailers will need access to consumers' identifying information (name, address, telephone number) from financial institutions in the case of electronically converted checks that were not collectable when presented through the ACH. The ability to retrieve identifying information from a financial institution in the case of an uncollected converted check is critical to the future growth of this form of payment and a reduction in paper checks. FMI encouraged the Board of Governors of the Federal Reserve to allow financial institutions to share identifying information under these circumstances as well as with other forms of payment processed through the ACH network and also to encourage and require the dissemination of this information.

Facilitating the electronic check conversion process will help achieve some of the most important goals of the financial privacy regulations. Specifically, the electronic check conversion process significantly reduces the amount of personally identifiable information that is held by an unaffiliated third party. Paper checks printed with name, address and telephone number are now no longer held by the retailer or the financial institution and instead are kept by the customer. Personally identifiable information would only be retrieved from the financial institution for the small number of electronically converted checks that are returned due to insufficient funds. Thus, encouraging electronic check conversion will further the overall goals of the financial privacy regulations.

1. Financial Privacy Restrictions Should Not Apply to Converted Check Transactions

Title V of the Gramm-Leach-Bliley Act contains several exclusions that should prevent the notice and non-disclosure requirements from applying in the case of converted checks that have been returned electronically due to insufficient funds (NSF). The statutory exclusions are reflected in proposed Section 313.10, "Exceptions to notice and opt out requirements for processing and servicing transactions." Specifically, proposed Section 313.10 states that the notice and opt out requirements would not apply to processing transactions at the consumer's request or to effect, administer or enforce a transaction requested or authorized by the consumer. The converted check example highlighted above is clearly authorized by the consumer and the information requested of the financial institution is clearly necessary to administer and enforce the transaction, thereby seeming to fall within the outlined exclusions.

Nonetheless, we have two specific concerns in this area. First, financial institutions should not only be allowed to share identifying information with retailers in the case of NSF checks that have been submitted electronically, financial institutions should be *required* to share this information as a standard practice. Second, in spite of the exclusions in Section 313.10, we are concerned that, without further clarification, financial institutions will simply opt not to supply the information due to confusion surrounding what information is allowed to be shared in this instance. In that case, the growth of electronically converted checks at the point-of-sale will be severely limited.

2. FTC Should Adopt Alternative "B" Definition of "Publicly Available Information"

The proposed rule sets forth two alternative definitions of "publicly available information." Under Alternative "A," information will not be considered "publicly available" unless the information is obtained from one of the public sources listed in the proposed rule. In contrast, Alternative "B" treats information as publicly available if it *could* be obtained from one of the public sources listed in the rules. Proposed Section 313.13(n-o-p); 65 Fed. Reg. at 11190-91.

Although the financial privacy restrictions should not apply in the converted check situation described above, the FTC should adopt the Alternative "B" definition of "publicly available information" because it would be helpful in encouraging financial institutions to continue to provide retailers with name, address and telephone information for consumers whose electronically converted checks have been returned unpaid due to insufficient funds. Alternative "A," which would require the financial institution to look up the name, address and phone number of a consumer in a telephone directory or other publicly available information source rather than to retrieve the same information from the account, would effectively put an end to the information sharing necessary for this new technology to succeed.

#### **D. Conclusion**

To summarize, we encourage the FTC to clarify the scope and definitions of the final rules to ensure that they apply only businesses that are significantly engaged in financial activities. Retailers, such as supermarkets who provide ATM access or money orders to consumers as ancillary services, are not "significantly engaged" in financial activities and, therefore, should not be considered "financial institutions" subject to the proposed rules. FMI and its members are concerned about privacy issues and have addressed the matter through the privacy policy that was adopted by the Board of Directors (copy enclosed).

Additionally, we strongly encourage the FTC to work with the Board of Governors of the Federal Reserve to not only allow, but to require as a standard business practice of financial institutions, the sharing of identifying information in the case of checks or other forms of payment processed through the ACH network that have been submitted electronically and then returned to the retailer due to insufficient funds. Our industry feels that this action would help us to reduce the increasing number of paper checks presented at retail stores and also the hundreds of millions of dollars in losses caused by returned checks at the retail level. Moreover, since retailers will not need to retain personally identifiable information for converted checks if this information can be readily obtained from financial institutions in those rare cases in which it is necessary, the overall goals of the financial privacy regulations will be furthered by ready retailer access to this information on an "as needed" basis.

\* \* \*

Secretary, Federal Trade Commission  
March 31, 2000  
Page 7

We appreciate the opportunity to provide comments on these important issues.  
Thank you for your consideration.

Sincerely,

A handwritten signature in black ink, appearing to read "G. R. Green", written over the typed name.

George R. Green  
Vice President  
General Counsel

Enclosure (1)



655 16TH STREET, N.W., SEVENTH FLOOR  
WASHINGTON, D.C. 20005-4707  
TELEPHONE: 202/452-6444  
FAX: 202/429-4519  
E-MAIL: FMI@FMI.ORG  
WEBSITE: WWW.FMI.ORG

## **FOOD MARKETING INSTITUTE POLICY STATEMENT ON CONSUMER PRIVACY**

**Adopted by FMI's Board of Directors**

**January 23, 2000**

We live in an era of unprecedented growth in the collection, dissemination and use of consumer data. Aggregate information derived from consumer purchases helps retailers and manufacturers better understand the needs of their customers, which, in turn, improves efficiency and lowers costs. Food retailers also have the ability to use personalized information as part of company marketing programs that benefit customers through special promotions, attractive merchandise discounts and new product offerings.

Despite these advantages, the collection and utilization of consumer data raises concern that the privacy of individual consumers could be compromised. Recognizing this concern early on, the Food Marketing Institute (FMI), a non-profit association representing more than 1,500 food retailers in the United States and around the world, developed a *voluntary* Policy Statement on Consumer Privacy in 1991. The policy was intended to provide guidance to members on integrating their business objectives with the privacy concerns of their customers in the rapidly expanding Information Age.

Information, in fact, is driving fundamental change in the relationship between retailers and their customers. While food retailing largely remains a mass merchandising industry, companies increasingly are able to utilize consumer purchase data to micro-market products and services to individual customers. Loyalty card or "frequent shopper" programs, which a number of retailers have implemented, offer special discounts and premium offers to customers who choose to participate. Another potential source of individualized service is the Internet, which largely is dependent upon information supplied by consumers about their product preferences, lifestyles, and other personal matters. Grocery store pharmacies offer retailers the opportunity to create targeted marketing, updates on medications and medical compliance programs (e.g., refill reminders) using prescription related data.

Retailers understand, and are sensitive to, the privacy issues arising in this new, data-rich environment. A number of companies, in fact, already have strong privacy policies in place. In the meantime, consumer privacy has become a cutting-edge issue for federal and state regulators, the news media and consumer organizations. In light of these developments, FMI has re-evaluated its 1991 Consumer Privacy Policy and is adopting an updated version designed to reassure customers that the industry remains committed to protecting consumer privacy in a rapidly changing world.



## POLICY

The Food Marketing Institute and its members support the consumer's right to privacy. It is the policy of the FMI Board that it is not appropriate to sell, rent, or relinquish personally identifiable information to third party vendors, suppliers, or marketers. FMI recognizes that transaction data is a resource that retailers can use on a confidential basis to improve customer service, lower costs and create personalized merchandising and marketing programs for their shoppers who desire to participate.

### Recommendation and Guidelines

The Food Marketing Institute recommends that each of its members adopt a customer privacy policy. FMI believes it is in the industry's best interest to develop a voluntary privacy standard that provides strong public assurance that the retail food industry is acting in good faith to protect the privacy of individual consumers.

The food retailing industry supports the following privacy guidelines:

- **Notice**

Retailers should inform their customers that information about their transactions is being tabulated and stored electronically in the retailer's databases and may be used internally as part of special merchandising and promotion programs. Customers also should know that the retailer may disclose non-personally identifiable compilations of information to third parties for marketing related purposes.

- **Choice**

Customers should be offered the opportunity to have their names removed from the retailer's database for internal marketing programs.

- **Security**

Companies must maintain strict procedures to prevent unauthorized access, alteration, or dissemination of personalized information. Customer data, even in the aggregate, should be restricted and accessible only to those employees with a "need to know" authorization.

- **Access**

Customers should have access (based upon written request) to any readily available and easily retrievable purchase information stored in retailer databases.

## **Confidentiality of Prescription Drug Records**

For those FMI members that operate in-store pharmacies, special consideration must be given to privacy issues related to personally identifiable medical or health information. The following additional guideline is intended for companies with pharmacies:

### **□ Patient Confidentiality**

Retailers and their pharmacies affirm that personal health and medical information is – and should be – private.

- FMI supports a uniform national medical confidentiality policy that permits the interchange of personally identifiable information among health care entities for purposes of professional treatment, insurance reimbursement, or improved health care outcomes.
- The presentation of a prescription by the patient, or request for prescription refill, is considered valid approval for the pharmacy to exercise its professional responsibilities, such as drug utilization review (DUR) and evaluation (DUE).
- Pharmacies will not transfer transaction data to third parties for marketing purposes without the express consent of customers. Customers should be offered the opportunity to have their names removed from the pharmacy database for internal marketing programs.

## **FMI Privacy Task Force**

### **Chairman:**

Norman Mayne  
Dorothy Lane Market, Inc.

### **Communications Committee**

Rita Owens, Publix Supermarkets, Inc.

### **Consumer Affairs Committee**

Joanie Taylor, Schnucks Markets, Inc.

### **Consumer Market Research Committee**

Lou Scudere, K-VA-T Food Stores, Inc.

### **Electronic Payment & Systems Committee**

Jacki Snyder, SUPERVALU, INC.

### **Government Relations Committee**

Dale Apley, Super Kmart

### **Independent Operator Committee**

Kevin Doris, Gerland's Food Fair, Inc.

### **Lawyers & Economists Committee**

Peter Phillipps, The Stop & Shop Supermarket Co.

### **Loss Prevention Committee**

Mike Harris, Hannaford Bros. Co.

### **Pharmacy Committee**

John Fegan, The Stop & Shop Supermarket Co.

### **Public Affairs Committee**

Jeff Gietzen, D&W Food Centers, Inc.

### **State Association Executive**

Peter Larkin, California Grocers Association